



Control Systems Security and Test Center

A Comparison of Electrical Sector Cyber Security Standards and Guidelines

***Prepared by the Idaho National Engineering
and Environmental Laboratory***



**Homeland
Security**



November 02, 2004

A Comparison of Electrical Sector Cyber Security Standards and Guidelines

November 2, 2004

**Control Systems Security and Test Center
Idaho Falls, Idaho 83415**

**Prepared for the
U.S. Department of Homeland Security
Under DOE Idaho Operations Office
Contract DE-AC07-99ID13727**

Control Systems Security and Test Center

A Comparison of Electrical Sector Cyber Security Standards and Guidelines

INEEL/EXT-04-02428

November 2, 2004

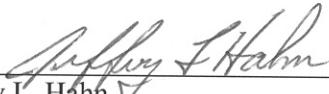
Approved by:



Robert P. Evans
Advisory Engineer

11-2-2004

Date



Jeffrey L. Hahn,
Lead Industry Liaison

11/2/2004

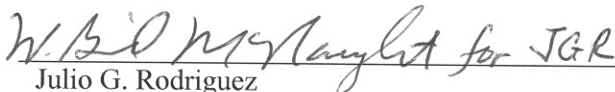
Date



Fred C. Cowart
Program Manager
Control Systems Security and Test Center

11-2-2004

Date



Julio G. Rodriguez
Department Manager
Critical Infrastructure Assurance

11-2-2004

Date



ABSTRACT

This report presents a review and comparison (commonality and differences) of five security standards and guidelines in the electrical distribution and control area. The comparison identifies security areas that are covered by each standard and/or guideline and reveals where the standards/guidelines differ in emphasis. By identifying differences in standards the user can evaluate which standards best meet their needs. For this report, only standards applicable to the electrical sector were reviewed.



CONTENTS

ABSTRACT.....	vii
ACRONYMS.....	xi
1. INTRODUCTION.....	1
2. PROBLEM.....	3
2.1 Applying Standards and Guidelines to Improve Security	3
3. STANDARDS	5
4. DISCUSSION - COMPARISON OF STANDARDS/GUIDELINES	7
5. CONCLUSIONS	9
6. REFERENCES	11
Appendix A Security Standards Comparison	13

TABLES

1. Major security sections in electrical sector standards.....	6
--	---





ACRONYMS

CAC	Cyber – Access Control
CBP	Continuity of Business Processes
CID	Cyber Intrusion Detection
CIF	Cyber IT Firewalls
CRM	Cyber – Risk Management
EBS	Employment Background Screening
EP	Emergency Plans
FY	Fiscal Year
HSPD	Homeland Security Presidential Directive
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Organization for Standardization
IT	Information Technology
NERC	North American Electric Reliability Council
PPSI	Protecting Potentially Sensitive Information
PS	Physical Security
SRA	Securing Remote Access to Electronic Control and Protection Systems
TIR	Threat and Incident Reporting
TR	Threat Response
VRA	Vulnerability and Risk Assessment



A Comparison of Electrical Sector Cyber Security Standards

1. INTRODUCTION

This report compares five standards and guidance documents aimed at improving security for the electrical industry. It includes a review of existing control system security standards and identifies potential guidelines for control system users. The Idaho National Engineering and Environmental Laboratory coordinated efforts with the Department of Energy's Critical Infrastructure Security Standards Working Group and academic partners at the University of Idaho to prepare this report.¹

Security in the context of this report encompasses both the physical and cyber protection of critical infrastructure. There are distinct differences in the topics considered by the current standards. Currently, the North American Electric Reliability Council (NERC) standards and guidelines focus on cyber security, while other industry standards, such as the Institute of Electrical and Electronics Engineers (IEEE) 1402 are more focused on physical security. However, there are many sections in each of the compared standards and guidelines that are similar. The purpose of this report is to promote an understanding of the electrical infrastructure security standards and guidelines, as an FY 2004 deliverable under the task "Promoting Existing Control System Security Standards and Guidelines."

There are other standards and guidelines relevant to physical and cyber security of electrical utility assets that have not been addressed here. It is recognized that standards and guidance documents are living documents that will continually evolve to meet the dynamic needs of industry and stay current with changing technology. While not enforceable, these documents represent industry best practices and when properly implemented, can provide for increased security to control systems.



2. PROBLEM

Many of the control systems operated by critical infrastructure in the United States are vulnerable to cyber intrusions that may impact normal operations, with consequences ranging from interruption of service and economic cost to catastrophic loss of life. The critical electrical infrastructure depends on complex interconnected control systems for its operation. In response to this risk, the President of the United States issued Homeland Security Presidential Directive (HSPD)–7 on December 17, 2003, which stated in part, “it is the policy of the United States to enhance the protection of our Nation’s critical infrastructure.” In addition, HSPD-7 states “The Department and Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms.”²

Physical and cyber attacks are increasing against the control systems used in our critical infrastructures.³ A recent U.S. General Accounting Office document cites several examples of such cyber attacks.⁴ There is usually property damage or personal injury involved with a physical attack and the news media will publicize the event. Cyber attacks on the other hand, are not as easily identified and many companies do not report the events and publicize their cyber vulnerabilities. Many of the cyber attacks may go unnoticed for long periods of time or not at all. However, the resources and tools for cyber attacks are becoming more commonplace and readily available. Many companies with assets that make up the critical infrastructure of the United States are largely unaware of the serious nature of the problem and hence have varying levels of cyber security designs and weak defenses in place.

Electronic intrusions and attacks may come from both inside and outside of a company. From within, intrusions may be innocent mistakes made by an operator, or deliberate attacks by disgruntled employees. Externally, intrusions may come from former employees, computer viruses or from hostile external attackers. HSPD-7 states, “While it is not possible to protect or eliminate the vulnerability of all critical infrastructure ... strategic improvements in security can make it more difficult for attacks to succeed and can lessen the impact of attacks that may occur.”² Cyber intrusions can be costly to industries, and many can be thwarted by applying cyber security standards and guidelines.

2.1 Applying Standards and Guidelines to Improve Security

Standards and guidelines can be used to help identify problems and reduce the vulnerabilities in a cyber security system. By knowing the problems and vulnerabilities, standards can be applied to cyber security systems to minimize both the risk and the consequences of intrusion. This report presents a comparison of some of the electrical sector cyber security standards and requirements. Using the proper standard for a particular industry’s application can reduce vulnerabilities in our nation’s critical infrastructure. For the electrical sector, this document helps identify which standard most closely matches that industry’s cyber security needs, and provides a tool for standards committees to consider the approach taken by other standards and guidelines.





3. STANDARDS

This section provides a brief description of the electrical sector security standards and guidelines used in this study. Table 1 shows the major sections of each standard. The scope of one standard may be focused on cyber security, while the scope of another standard may be physical security, or communications. This study can help identify the similarities and differences between standards and guidelines, which can contribute to selecting the best security practices and help strengthen sections of the standards and guidelines in future revisions.

1. The International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 17799, Information Technology—Code of Practice for Information Security Management (ISO 17799) is a detailed security standard, organized into ten major sections.⁵

Although it was not written specifically for the electrical sector, ISO 17799 may be regarded as a starting point for developing organization guidance. It offers guidelines and voluntary directions for information security management and is meant to provide a general description of the areas currently considered important when initiating, implementing, or maintaining information security in an organization.⁶

2. IEEE 1402, IEEE Guide for Electric Power Substation Physical and Electronic Security⁷ is a guide sponsored by the Power Engineering Society/Substations of IEEE. It was approved June 7, 2000. The guide identifies and discusses security issues related to human intrusion at electric power supply substations. Various methods and techniques that are being used to mitigate physical and electronic intrusions are presented.
3. The NERC Security Guidelines for the Electricity Sector⁸ is published by the North American Electric Reliability Council. Version 1.0 was released June 14, 2002. The guideline consists of 14 sections addressing physical and cyber security.

These guidelines describe general approaches, considerations, practices, and planning philosophies to be applied in protecting the electric infrastructure systems. The guidelines are advisory in nature and it is left to each company to determine how they will be used.⁹

4. NERC 1200, Urgent Action Standard 1200 – Cyber Security is a temporary standard published by the North American Electric Reliability Council (NERC) to establish a required set of defined security requirements relative to the electrical utility industry and to reduce risks to the reliability of the bulk electric systems from any compromise of critical cyber assets.¹⁰ This standard was adopted August 13, 2003, for a one-year period. It has received an extension, until August 2005, at which time a permanent Cyber Security Standard (NERC 1300) is expected to be released.¹¹

This standard, organized into 16 major sections, applies to entities performing various electric system functions, as defined in the functional model approved by the NERC Board of Trustees in June 2001. NERC is now developing standards and procedures for identifying and certifying such entities. Until that identification and certification is complete, these standards apply to the existing entities (such as control areas, transmission owners and operators, and generation owners and operators) that are currently performing the defined functions.¹²

5. NERC 1300, Cyber Security¹³ is proposed to replace the NERC 1200.¹⁴ The North American Electric Reliability Council is preparing NERC 1300. Draft 1 of the Cyber Security Standard was posted for comment September 15 through November 1, 2004. This standard is expected to cover essentially the same material as NERC 1200, but in more detail. It is currently organized in eight major sections.

Table 1. Major security sections in electrical segment standards and guidelines.

ISO 17799 82 pages	IEEE 1402 24 pages	NERC Security Guidelines for the Electricity Sector 73 pages	NERC 1200 24 pages	NERC 1300 Draft 1.0 September 15, 2004 35 pages
Security Policy	Intrusions	Vulnerability and Risk Assessment	Cyber Security Policy	Security Management Controls
Organizational Security	Criteria for Substation Security	Threat Response	Critical Cyber Assets	Critical Cyber Assets
Asset Classification and Control	Security Methods, Barriers, Electronic, Other	Emergency Plans	Electronic Security Perimeter	Personnel and Training
Personnel Security	Effectiveness of Security Methods	Continuity of Business Processes	Electronic Access Controls	Electronic Security
Physical and Environmental Security	Substation Security Plan	Communications	Physical Security Perimeter	Physical Security
Communications and Operations Management		Physical Security	Physical Access Controls	Systems Security Management
Access Control		Cyber – Risk Management	Personnel	Incident Response Planning
Systems Development and Maintenance		Cyber – Access Control	Monitoring Physical Access	Recovery Plans
Business Continuity Management		Cyber – IT Firewalls	Monitoring Electronic Access	
Compliance		Cyber – Intrusion Detection	Information Protection	
		Employment Background Screening	Training	
		Protecting Potentially Sensitive Information	Systems Management	
		Securing Remote Access to Electronic Control and Protection Systems	Test Procedures	
		Threat and Incident Reporting	Electronic Incident Response Actions	
			Physical Incident Response Actions	
			Recovery Plans	



4. DISCUSSION - COMPARISON OF STANDARDS/GUIDELINES

Appendix A is a matrix that compares the five standards/guidelines considered in this report. International standard ISO 17799 was used as the baseline because it appears to have the broadest coverage. By examining Appendix A, it is possible to see how the sections of these particular standards or guidelines address the sections within ISO 17799. The standards/guidelines were compared in the following areas:

- Security Policy
- Vulnerability and Risk Assessment
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance

Since all of the standards do not address the same requirements, it is recognized that there will be areas where there are no comparisons. For example, IEEE 1402 is geared more toward physical security, while the NERC standards and guidelines focus on the cyber security aspect. The ISO standard considers the network, operating system, and application separately, and looks at requirements such as passwords for each of these individually. The other standards consider passwords and then assume that any item that could use password protection is covered. This leads to difficulty in comparing standards and leaves the comparison open to interpretation.



5. CONCLUSIONS

This report reviews and compares the content of five security standards/guidelines used in the electrical sector. There are distinct differences in the topics considered by some of the standards/guidelines. Therefore, a careful examination of this comparison and of the standards/guidelines included here should be made before attempting to use any given standard/guideline.

It is recognized that there are other applicable standards/guidelines, such as IEC 61850, IEC 60870-6 (TASE.2) and DNP 3.0, which have not been addressed here. Groups that are actively working on standards/guidelines related to the cybersecurity of electrical infrastructure include the International Electrotechnical Commission (IEC) Technical Committee (IEC TC 57) Working Group 15, IEC TC 66, CIGRE, IEEE C1 and ISA SP99.





6. REFERENCES

1. Schmidt, J. and Nair, V., *A Taxonomy of Security Standards for Real-Time Control Systems*, 2004.
2. December 17, 2003 Homeland Security Presidential Directive/HSPD-7, Critical Infrastructure Identification, Prioritization, and Protection, <http://www.whitehouse.gov/news/releases/2003/12/print/20031217-5.html>
3. Poulsen, K., "Shifting Cyber Threats Menace Factory Floors," *Security Focus Printable NEWS* 9671, October 7, 2004, <http://www.securityfocus.com/news/9671>
4. U. S. General Accounting Office, 2004, *Critical Infrastructure Protection - Challenges and Efforts to Secure Control Systems*, GAO-04-354, U. S. General Accounting Office, March, <http://www.gao.gov/>
5. ISO17799 Made Easy, ISO/IEC 17799 Security Resources, <http://www.iso-17799-security-world.co.uk/>
6. ISO/IEC 17799:2000, "Code of Practice for Information Security Management, Frequently Asked Questions," *What is ISO/IEC 17799:2000?*, November 2002, <http://csrc.nist.gov/publications/secpubs/otherpubs/reviso-faq.pdf>
7. IEEE Standard 1402-2000, *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE, Inc. 3 Park Avenue, New York, NY 10016-5997.
8. NERC Security Guideline, *Securing Remote Access to Electronic Control and Protection Systems*, June 12, 2003, Version 1.0, www.esisac.com/publicdocs/Guides/secguide_pcs_final.pdf (5 March 2004).
9. Security Guidelines for the Electricity Sector, Overview, Version 1.0, <http://www.esisac.com/publicdocs/Guides/SecurityGuidelinesElectricitySector-Version1.pdf>
10. NERC 1200 Cyber Security, ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStd-3-3121.pdf
11. NERC Approves Extension of Urgent Action Cyber Security Standard, NERC News, September 8, 2004, <http://www.nerc.com/~filez/nercnews/news-0804c.html>
12. "Key Energy and Utility Security Questions," *What is the NERC 1200 Urgent Action Cyber Security Standard?*, Breakwater Security Associates, http://www.breakwatersecurity.com/energy/key_questions.html?id=2
13. NERC 1300, Draft 1.0, ftp://www.nerc.com/pub/sys/all_updl/standards/sar/Draft_Version_1_Cyber_Security_Standard_1300_091504.pdf
14. NERC Standards Development Bulletin, September 2004, <http://www.nerc.com/~filez/standards/standards-bulletin-0904.htm>





Appendix A

Security Standards Comparison



Appendix A

Security Standards Comparison

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>SECURITY POLICY</u>	3	8, 8.1, 8.3, 8.5		1201	1301
Information security policy.	3.1		PPSI	1201.1.1	1301.a, 1301.b
Information security policy document.	3.1.1				1301.a.1, 1301.a.2, 1301.b.1.i
Review and evaluation of information security policy.	3.1.2		Overview. P2, TR.TC-N.10, SRA.P3.1	1201.2.2	1301.b.1.ii, 1301.b.1.iv, 1301.b.2.i, 1301.b.2.iv, 1301.b.3.iv, 1301.b.4, 1305.b.1

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>VULNERABILITY AND RISK ASSESSMENT</u>			VRA		1302
Vulnerability and risk assessment.			VRA		1302
Conduct a risk assessment.	7.1.1, 7.1.5, 7.2.5, 7.2.6, 9.4.3, 9.7.2.1, 10.2, 10.3.1, 10.3.2, 11.1.2	5	VRA	1212.1.11	1302.a, 1302.b.2, 1306.a.5, 1306.b.5
Risk management process.			VRA, CRM		
Mitigation program.		5	VRA.P4, EP.P2, CRM		
Equipment backup			TR.TC-N.12, TR.TC-M.8, EP.P2		
General considerations for conducting a risk and vulnerability assessment.			VRA.P3-4		

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>ORGANIZATIONAL SECURITY</u>	4				1301
Information security infrastructure.	4.1				1301.a
Management information security forum.	4.1.1				1301.a.3
Information security coordination (within the organization).	4.1.2				1301.a.4
Allocation of information security responsibilities (for assets and processes including leadership and management).	4.1.3	8.2	VRA.P3	1201.1.2, 1201.2.3, 1201.2.4	1301.a.3, 1301.a.4
Authorization process for new information processing facilities.	4.1.4				
Specialist information security advice.	4.1.5				
Cooperation between organizations.	4.1.6		VRA.P4, C.P2.1-7		
Restrict exchanges of sensitive information.	4.1.6		C.P3.9, PPSI.P3		
Respond to disclosures of sensitive information.			PPSI.P4		
Independent review of information security.	4.1.7				
Security of third party access.	4.2				
Identification of risks from third party access.	4.2.1				
Types of access (physical or logical).	4.2.1.1				
Reasons for access.	4.2.1.2				
On-site contractors.	4.2.1.3				
Security requirements in third party contracts.	4.2.2				
Outsourcing.	4.3				
Security requirements in outsourcing contracts.	4.3.1				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>ASSET CLASSIFICATION AND CONTROL</u>	5			1202	1302
Accountability for assets.	5.1				
Inventory of assets.	5.1.1			1202.1, 1202.2.1-2.2, 1205.2.1	1302.a, 1302.b, 1305
Information classification.	5.2				
Classification guidelines.	5.2.1				
Information labeling and handling.	5.2.2				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>PERSONNEL SECURITY</u>	6			1207	1303
Security in job definition and resourcing.	6.1				
Including security in job responsibilities.	6.1.1	6.3.6.1			
Personnel (background) screening and policy.	6.1.2		EBS.P1-2	1207.2.3	1303.a.3-4, 1303.b.3-4
Confidentiality agreements.	6.1.3				
Terms and conditions of employment.	6.1.4				
Identify personnel granted physical or electronic access.				1207.1, 1207.2.1, 1207.2.2	1303.a.3, 1303.b.3
Department employees and contractors					1303.a.4, 1303.b.4

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
User training.	6.2			1211	1303
Information security education, training, and awareness.	6.2.1	6.3.6.1	Overview.p4, TR.TC-N.8, TR.TC- L.3, TR.TC-M.2, TR.TC-H.3, EP.P2, PPSI, C.P3.8-9, PS.P3, PPSI.P4	1211.1, 1211.2.1-2.1.5	1303.a.1-3, 1303.b.1-3, 1308.a.4, 1308.b.4
Responding to security incidents and malfunctions.	6.3		EP	1214.1 1214.2.1-2.2, 1215.1, 1215.2.1-2.2	1307.a, 1307.b
Reporting security threats, incidents, and weaknesses.	6.3.1, 6.3.2	8.2, 6.3.6.2	TR.TC-N.7, TR.P2- 7, TIR	1214.2.2	1307.a.4, 1307.b.3
Timely reporting.	6.3.1		TR.P2-7, TIR.P3		
Information to report.			TIR.P4		
Incident reporting mechanisms.	6.3.1	6.3.6.2	TR.P2-7, TIR.P6	1214.2.2	1307.a.4, 1307.b.3
Reporting software malfunction.	6.3.3				
Learning from incidents.	6.3.4	6.3.6.1	EP.P3&P4		
Disciplinary process.	6.3.5				
Threat response (enhanced security) related to announced threat levels.			TR		
Threat response level suggested elements (four Threat Con alert levels: normal, low, medium, high).			TR		

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>PHYSICAL AND ENVIRONMENTAL SECURITY</u>	7		PS	1205	1305
Secure areas.	7.1				
Physical security perimeter.	7.1.1	6.1.1, 6.1.2, 6.1.3 6.1.4, 6.2, 6.2.1	TR.TC-N.12, PS.P2-3	1205.1, 1205.2.1-2.2	1305.a.2, 1305.b.2
Monitoring physical access.	7.1.1	6.2.2, 6.2.3	PS.P2-3, CAC.Monitoring	1208.1, 1208.2.1-2.2	1305.a.4, 1305.b.4-5
Physical entry controls	7.1.2		TR.P2-7, PS.P2-3	1206.1, 1206.2.1-2.2	1305.a.3, 1305.b.3
Securing offices, rooms, and facilities.	7.1.3		TR.P2-7, PS.P2-3		
Working in secure areas.	7.1.4		TR.P2-7, PS.P2-3		
Isolated delivery and loading areas.	7.1.5		TR.P2-7, PS.P2-3		
Intruder detection	7.1.3.e		PS.P2-3		1305.a.6
Other physical security methods.		6.3.1, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.7	PS.P2-3		
Equipment security.	7.2		PS.P2-3		
Equipment siting and protection.	7.2.1				
Power supplies.	7.2.2				
Cabling security.	7.2.3				
Equipment maintenance.	7.2.4				
Security of equipment off-premises.	7.2.5				
Secure disposal or re-use of equipment.	7.2.6				
General controls (information and information processing facilities).	7.3				
Clear desk and clear screen policy.	7.3.1				
Removal of property.	7.3.2				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>COMMUNICATIONS AND OPERATIONS MANAGEMENT</u>	8				
Operational procedures and responsibilities.	8.1				
Documented operating procedures.	8.1.1				
Operational change control.	8.1.2				1306.a.7, 1306.b.7
Incident management procedures.	8.1.3		TIR.P3, TIR.P4, TIR.P6, TR.P2-7		1307.a, 1307.b
Segregation of duties.	8.1.4				
Separation of development and operational facilities.	8.1.5				
External facilities management.	8.1.6				
Testing and documentation procedure				1213.1, 1213.2.1-2.2	1306.a.1, 1306.b.1
System planning and acceptance.	8.2				
Capacity planning.	8.2.1				
System acceptance.	8.2.2			1213.1, 1213.2.1-2.2	1306.a.1, 1306.b.1
Protection against malicious software.	8.3				1306.a.4
Controls against malicious software.	8.3.1	6.2.4.4	CIF.P1, CID.P1	1212.1.9	1306.b.4
Operating status monitoring					1306.a.10, 1306.b.10
Vulnerability assessment (controlled penetration testing)					1306.a.5, 1306.b.5
Housekeeping.	8.4				
Information back-up.	8.4.1				1306.a.11, 1306.b.11
Operator logs.	8.4.2				
Fault logging.	8.4.3				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
Network management.	8.5				
Network controls.	8.5.1				
Media handling and security.	8.6				
Management of removable computer media.	8.6.1				
Disposal of media.	8.6.2, 7.2.6				
Information handling procedures.	8.6.3				
Information protection.				1210.1, 1210.2.1-2.2	1301.a.2, 1301.b.2
Security of system documentation.	8.6.4				
Exchanges of information and software.	8.7		C.P3.9, PPSI.P3		
Information and software exchange agreements.	8.7.1				
Security of media in transit.	8.7.2				
Electronic commerce security.	8.7.3				
Security of electronic mail: security risks and policy on electronic mail.	8.7.4, 8.7.4.1, 8.7.4.2				
Security of electronic office systems.	8.7.5				
Publicly available systems.	8.7.6				
Other forms of information exchange.	8.7.7				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>ACCESS CONTROL</u>	9		CAC	1204, 1206	1304
Business requirements for access control.	9.1		CAC Authorization		1304
Access control policy.	9.1.1		CAC. Guideline Statement		
Policy and business requirements.	9.1.1.1		CAC. Authorization, SRA.P3-4		1304.a
Access control rules.	9.1.1.2		CAC. Authorization, SRA.P3-4		1304.a.2
User access management.	9.2		CAC	1204, 1206	1306.a.2, 1306.b.2
User registration.	9.2.1		CAC .Authorization, SRA.P3.6	1212.1.2-1.3	1301.a.5, 1301.b.5, 1306.a.2, 1306.b.2
Privilege management.	9.2.2				
Authentication.			CAC. Authentication, SRA.P3.3		1306.a.2
User password management.	9.2.3		CAC. Authentication, SRA.P3.4, SRA.P3.7, SRA.P4.11	1212.1.1	1306.a.2, 1306.b.2
Review of user access rights.	9.2.4		CAC. Authorization, SRA.P3.6	1212.1.2	1301.a.5.iii, 1301.b.5
User responsibilities.	9.3		CAC		
Password use.	9.3.1	6.2.4.1	CAC.Authentication, SRA.P3.7, SRA.P4.11.B		
Unattended user equipment (protection).	9.3.2				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
Network access control.	9.4				
Policy on use of network services.	9.4.1				
Enforced path.	9.4.2				
Selective access		6.2.4.3			
Securing remote access.		6.2.4.2	SRA	1212.1.4-5	1306.a.8-9, 1306.b.8-9
User authentication for external connections.	9.4.3		SRA.P3.2-4, SRA.P2.GS, SRA.P4.11		
Node authentication.	9.4.4		SRA.P4.11.C-D		
Remote diagnostic port protection.	9.4.5		SRA.P3.2, SRA.P4.11	1212.1.5	1306.a.9
Segregation in networks. (Cyber – IT Firewalls)	9.4.6		CIF	1212.1.6	
Network connection control.	9.4.7			1212.1.4-5	1306.a.8-9, 1306.b.8-9
Network routing control.	9.4.8				
Security of network services (description of services security attributes).	9.4.9				
Identify electronic security perimeter.				1203.1, 1203.2.1-2.2	1304.a.1, 1304.b.1
Electronic access controls.				1204.1, 1204.2.1-2.2	1304.a.2-3, 1304.b.2-3
Operating system access control.	9.5		CAC, SRA	1204	1304, 1306
Automatic terminal identification.	9.5.1				
Terminal log-on procedures.	9.5.2				
User identification and authentication.	9.5.3		CAC. Authentication, SRA.P3.3		1306.a.2

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
Password management system.	9.5.4		CAC. Authentication, SRA.P3.4, SRA.P3.7, SRA.P4.11	1212.1.1	1306.a.2, 1306.b.2
Use of system utilities.	9.5.5				
Duress alarm to safeguard users.	9.5.6				
Terminal time-out.	9.5.7				
Limitation of connection time.	9.5.8				
Application access control.	9.6		CAC, SRA	1204	1304, 1306
Information access restriction.	9.6.1				
Sensitive system isolation.	9.6.2				
Monitoring system access and use.	9.7				
Event logging.	9.7.1		CAC.Monitoring, CID.P1	1212.1.10	1306.a.6, 1306.b.6, 1306.a.10, 1306.b.10
Monitoring system use/access.	9.7.2		CAC.Monitoring, CID.P1	1209.1, 1209.2.1-2.2	1304.a.3, 1304.b.3
Procedures (for monitoring use including intrusion detection systems) and areas of risk.	9.7.2.1			1212.1.7	1304.a.3, 1304.b.3
Review results of monitoring activities based on risk factors.	9.7.2.2				
Logging and reviewing events (emphasis on review).	9.7.2.3		CIF.P1, CID.P1	1212.1.10	
Clock synchronization.	9.7.3				
Mobile computing and teleworking considerations.	9.8, 9.8.1, 9.8.2				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>SYSTEMS DEVELOPMENT AND MAINTENANCE</u>	10				
Security requirements of systems.	10.1				
Security requirements analysis and specification.	10.1.1				
Systems management policies and procedures.				1212.1	1306.a, 1306.b
New systems and significant changes to existing systems must use information security test procedures.					1306.a.1, 1306.b.1
Security in application systems.	10.2				
Input data validation.	10.2.1				
Control of internal processing.	10.2.2				
Areas of risk.	10.2.2.1				
Checks and controls.	10.2.2.2				
Message authentication. (see 10.3.2)	10.2.3				
Output data validation.	10.2.4				
Cryptographic controls.	10.3				
Policy on the use of cryptographic controls.	10.3.1				
Encryption.	10.3.2	6.2.4.5	SRA.P3.5		
Digital signatures considerations.	10.3.3				
Non-repudiation services.	10.3.4				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
Key management.	10.3.5				
Protection of cryptographic keys.	10.3.5.1				
Standards, procedures, and methods.	10.3.5.2				
Security of system files.	10.4				
Control of operational software.	10.4.1				
Protection of system test data.	10.4.2				
Access control to program source library.	10.4.3				
Security in development and support processes.	10.5				
Change control procedures.	10.5.1				1306.a.7, 1306.b.7
Technical review of operating system changes.	10.5.2				1306.a.1, 1306.b.1, 1306.a.3, 1306.b.3
Restrictions on changes to software packages.	10.5.3				
Covert channels and Trojan code considerations.	10.5.4				
Outsourced software development considerations.	10.5.5				
Security patch management.				1212.1.8	1306.a.3, 1306.b.3

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>BUSINESS CONTINUITY MANAGEMENT</u>	11				1308
Aspects of business continuity management.	11.1				
Business continuity management process.	11.1.1		VRA.P4, EP.P2-4, CBP		
Business continuity and impact analysis.	11.1.2				
Writing and implementing continuity plans.	11.1.3		CBP	1216.1, 1216.2.1	1308.a 1308.b
Business continuity planning framework (consistency of plans).	11.1.4		CBP		
Testing, maintaining, and re-assessing business continuity plans.	11.1.5, 11.1.5.1- 11.1.5.2		EP.P2-4, CBP.P3	1216.2.2	1308.a.1, 1308.a.3, 1308.b.1, 1308.b.3

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
<u>COMPLIANCE</u>	12				
Compliance monitoring process (compliance with standard).				1201-1216.4.1-4.3	1301-1308.d-f
Inspection of facilities.		8.2			
Compliance with legal requirements.	12.1		Overview.P4		
Identification of applicable legislation.	12.1.1				
Intellectual property rights: copyright, software copyright.	12.1.2, 12.1.2.1- 12.1.2.2				

Requirement	ISO 17799	IEEE 1402	NERC Security Guideline for the Electricity Sector *	NERC 1200	NERC 1300 Draft 1.0 September 15, 2004
Safeguarding of organizational records.	12.1.3				
Data protection and privacy of personal information.	12.1.4				
Prevention of misuse of information processing facilities.	12.1.5				
Regulation of cryptographic controls.	12.1.6				
Collection of evidence: rules for evidence, admissibility of evidence, quality of evidence.	12.1.7, 12.1.7.1-12.1.7.3				
Reviews of security policy and technical compliance.	12.2		TR.TC-N.10		1301-1308.d
Compliance with security policy (auditing)	12.2.1		TR.TC-N.9, SRA.P3.8		1301-1308.d.1
Technical compliance checking.	12.2.2				1306.a5, 1306.b.5
System audit considerations.	12.3				
System audit controls.	12.3.1				
Protection of system audit tools.	12.3.2				

Key to Abbreviations for Security Guidelines for the Electricity Sector:

VRA	Vulnerability and Risk Assessment V1.0 June 14, 2002	PS	Physical Security V1.0 June 14, 2002	PPSI	Protecting Potentially Sensitive Information V1.0 June 14, 2002
TR	Threat Response V1.0 June 14, 2002	CRM	Cyber – Risk Management V1.0 June 14, 2002	SRA	Securing Remote Access to Electronic Control and Protection Systems V1.0 June 10, 2003
EP	Emergency Plans V1.0 June 14, 2002	CAC	Cyber – Access Control V1.0 June 14, 2002	TIR	Threat and Incident Reporting V1.0 June 10, 2003
CBP	Continuity of Business Processes V1.0 June 14, 2002	CIF	Cyber IT Firewalls V1.0 June 14, 2002		
C	Communications V1.0 June 14, 2002	CID	Cyber Intrusion Detection V1.0 June 14, 2002		
		EBS	Employment Background Screening V1.0 June 14, 2002		